NetSPI™

API Penetration Testing

Secure your APIs against evolving threats with actionable insights discovered through expert-led penetration testing aligned with OWASP API Security Top 10.

NetSPI evaluates target APIs across the entire API stack, testing both authenticated and unauthenticated access scenarios to help your security and development teams inventory and evaluate APIs for security vulnerabilities. Our comprehensive approach combines manual expertise with automated tools to identify critical vulnerabilities including injection flaws, broken authentication, authorization bypasses, and business logic vulnerabilities that could compromise your applications and data.

5 Key Testing Focus Areas

1. **Authentication & Authorization Flaws**
   We rigorously test authentication mechanisms and authorization controls to identify bypasses, including broken object-level authorization, function-level access control issues, JWT and access token vulnerabilities, and credential management weaknesses.
2. **Injection Vulnerabilities**
   Our team identifies SQL, NoSQL, and command injection vulnerabilities that could allow attackers to manipulate queries, bypass authentication, access unauthorized data, or compromise backend systems.
3. **Data Exposure & Privacy**
   We assess APIs for excessive data exposure, sensitive information disclosure in responses, and broken object property level authorization that could leak passwords, tokens, PII, or business-critical data.
4. **Business Logic & Rate Limiting**
   Testing goes beyond common vulnerabilities to identify unrestricted resource consumption, business logic flaws, and missing rate limiting that could lead to denial of service or abuse of sensitive business flows.
5. **Security Misconfigurations**
   We evaluate your API infrastructure for common misconfigurations including verbose error messages enabling user enumeration, improper inventory management, unsafe third-party API consumption, and SSRF vulnerabilities.

Comprehensive Testing Methodology

Information Gathering

- API catalog walkthrough and documentation review
- Architecture and business logic analysis
- Test plan development aligned with your risk priorities
- Credential and scope validation

Testing & Evaluation

- Anonymous and authenticated user testing
- Manual and automated vulnerability assessment
- Data flow and business logic analysis
- Access control verification across all user roles
- OWASP API Top 10 comprehensive coverage

Analysis & Reporting

- CVSS v3.1 scoring and category mapping to the OWASP API Top 10 for all findings
- Business impact assessment
- Specific remediation guidance
- Technical verification evidence
- Executive summary and detailed findings context

Tackle Your Security Goals with a Trusted Team

Collaboration is one of NetSPI's core values. We work with you to ensure that findings are analyzed, communicated, and remediated in alignment with compliance requirements and your strategic business or program goals.

Real-Time Reporting – Get notified of vulnerabilities in-platform as they are found.

Remediation Guidance – Vulnerabilities are delivered with detailed remediation instructions and consultant support.

Project Management & Communication – Effortlessly assign responsibilities, track remediation status, communicate with teams, and more.

Track & Trend Data – Analyze findings and discover trends over time across multiple assessments.

To learn more about NetSPI's solution offerings, visit www.netspi.com or contact us.

NetSPI™

NetSPI PTaaS

Penetration Testing

Application Pentesting

- Web Application
- Mobile Application
- Thick Application
- Virtual Application
- API
- SBOM
- CI/CD Pipeline

Network Pentesting

- Internal Network
- External Network
- Wireless Network
- Host-Based
- Mainframe

AI/ML Pentesting

- LLM Web App
- LLM Benchmark/ Jailbreak

Cloud Pentesting

- AWS
- Azure
- Google Cloud
- Kubernetes

Mainframe

- ZSeries (z/OS)
- IBMi (as400)
- HP Nonstop

Hardware & IoT

- IoT/OT
- ATM
- Automotive
- Medical Device
- Embedded

Security Assessments

Red Team

- Assumed Breach
- Scenario Based
- Black Box
- Threat Intel Led (DORA)

Detective Controls Validation

- Azure
- Windows
- Linux
- MacOS
- ESXi
- And more

Social Engineering

- Phishing
- Vishing
- Physical Pentest
- On-site Assessment

Threat Modeling

- STRIDE, PASTA, and Proprietary

Blockchain Pentesting

- Smart Contract Audit
- Infrastructure Test
- Web Application Test

Secure Code Review

- SAST & SCR
- SAST Triaging

You Deserve The NetSPI Advantage

Human Driven

- **350+ pentesters**
- **Employed, not outsourced**
- **Wide domain expertise**

AI-Enabled

- **Consistent quality**
- **Deep visibility**
- **Transparent results**

Modern Pentesting

- **Use case driven**
- **Friction-free**
- **Built for today's threats**

About NetSPI

NetSPI® pioneered Penetration Testing as a Service (PTaaS) and leads the industry in modern pentesting. Combining world-class security professionals with AI and automation, NetSPI delivers clarity, speed, and scale across 50+ pentest types, attack surface management, and vulnerability prioritization. The NetSPI platform streamlines workflows and accelerates remediation, enabling our experts to focus on deep dive testing that uncovers vulnerabilities others miss. Trusted by the top 10 U.S. banks and Fortune 500 companies worldwide, NetSPI has been driving security innovation since 2001. NetSPI is headquartered in Minneapolis, MN, and available on **AWS Marketplace**. Follow us on **LinkedIn** and **X**.